UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/405,031	09/24/1999	DOUGLAS R. COFFLAND	IL-10360	9034

7590 07/29/2004

LLOYD E DAKIN JR
ASSISTANT LABORATORY COUNSEL
LAWRENCE LIVERMORE NATIONAL LABORATORY
P O BOX 808-L-703
LIVERMORE, CA 94551

EXAMINER	
BETIT, JACOB F	

ART UNIT	PAPER NUMBER
2175	

DATE MAILED: 07/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/405,031	COFFLAND, DOUGLAS R.D	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 13 May 2004 has been entered.

Remarks

2. In response to communications filed on 13 May 2004, claims 1, 10, 17, and 24 are amended per applicant's request. Claims 1-30 are presently pending in the application.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 is rejected because it includes both the limitation "means for compressing a media signal" and the limitation "data compression means coupled to receive and compress the

media signal". It is unclear from reading the claim whether the "means for compressing" and the "data compression means" are the same means for compressing one signal, the same means for compressing two different signals, two different means for compressing the same signal, or two different means for compressing two different signals. For the purpose of examining it is assumed that there is one compressing means for compressing one signal.

Claims 2-9 are rejected for being dependant on rejected independent claim 1.

Appropriate corrections are required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5, 7, 9-14, 16-21, 23-28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Koopman, Jr. (U.S. patent No. 5,757,923, and in further view of Borza et al. (U.S. patent No. 6,215,874 B1).

As to claim 1, Noll et al. teaches a system for multimedia encryption comprising:

a media signal (see column 4, lines 58-66);

data acquisition means coupled to receive and select a set of data from the data stream (see figure 1, steps 100 and 105); and

hashing coupled means to receive and hash the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach means for compressing a media signal; data compression means coupled to receive and compress the media signal into a compressed data stream; and set of data from the compressed data stream.

Koopman, Jr. teaches generating secret identification numbers from a random digital data stream (see abstract), in which he teaches means for compressing a media signal; data compression means coupled to receive and compress the media signal into a compressed data stream; and set of data from the compressed data stream (see column 7, lines 1-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include means for compressing a media signal; data compression means coupled to receive and compress the media signal into a compressed data stream; and set of data from the compressed data stream.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because means for compressing a media signal; data compression means coupled to receive and compress the media signal into a compressed data stream; and set of data from the compressed data stream would improve the entropy per bit which would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

Noll et al. as modified, still does not teach said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; the media signal containing random noise that is completely unpredictable from one moment to the next.

Borza et al. teaches generating random numbers using imaging transducers of a charge coupled array (see abstract), in which he teaches said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; the media signal containing random noise that is completely unpredictable from one moment to the next (see column 6, lines 5-33).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; the media signal containing random noise that is completely unpredictable from one moment to the next.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Borza et al. because said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; the media signal containing random noise that is completely unpredictable from one moment to the next would produce a random number to be used as a seed in a pseudo random number generator (see column 10, lines 4-12).

As to claim 2, Noll et al. as modified, teaches wherein the set of data is one frame of data within the compressed data stream (see Noll et al., column 4, lines 61-62).

As to claim 3, Noll et al. as modified, teaches wherein the set of data crosses over several frame boundaries within the compressed data stream (see Noll et al., column 4, lines 60-61).

As to claim 7, Noll et al. as modified, teaches wherein the media signal includes a noise signal amplitude (see Borza et al., column 5, lines 4-16);

further comprising,

an analog to digital converter, having a quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal (see Borza et al., column 6, lines 21-33); and

wherein the data compression module compresses the quantized media signal into a compressed data stream (see Koopman, Jr., column 7, lines 1-59).

As to claim 9, Noll et al. as modified, teaches further comprising:

a pseudo-random number generator coupled to receive and process the keyword in to a set of keywords (see Noll et al., column 4, lines 23-26).

As to claim 10, Noll et al. teaches a method for multimedia encryption, comprising the steps of:

a media signal (see column 4, lines 33-55);

selecting a set of data from the media signal (see figure 1, steps 100 and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach compressing a media signal; and a set of data from the compressed media signal.

Koopman, Jr. teaches compressing a media signal; and a set of data from the compressed media signal (see column 7, lines 1-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include compressing a media signal; and a set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because compressing a media signal; and a set of data from the compressed media signal would improve the entropy per bit which would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

Noll et al. as modified, still does not teach said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

Borza et al. teaches said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 6, lines 5-33).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include said media

signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Borza et al. because said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next would produce a random number to be used as a seed in a pseudo random number generator (see Borza et al., column 10, lines 4-12).

As to claim 17, Noll et al. teaches a system for multimedia encryption, comprising:

a media signal (see column 4, lines 33-55);

means for selecting a set of data from the media signal (see figure 1, steps 100 and 105); and

means for hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" reads on "seed").

Noll et al. does not teach means for compressing a media signal; and a set of data from the compressed media signal.

Koopman, Jr. teaches teach means for compressing a media signal; and a set of data from the compressed media signal (see column 7, lines 1-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include teach means for compressing a media signal; and a set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because teach means for compressing a media signal; and a set of data from the compressed media signal would improve the entropy per bit which would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

Noll et al. as modified, still does not teach said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

Borza et al. teaches said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 6, lines 5-33).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Borza et al. because said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next would produce a random number to be used as a seed in a pseudo random number generator (see Borza et al., column 10, lines 4-12).

As to claim 24, Noll et al. teaches a computer-useable medium embodying computer program code for multimedia encryption by executing the steps of:

a media signal (see column 4, lines 33-55);

selecting a set of data from the media signal (see figure 1, steps 100 and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach compressing a media signal; and a set of data from the compressed media signal.

Koopman, Jr. teaches compressing a media signal; and a set of data from the compressed media signal (see column 7, lines 1-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include compressing a media signal; and a set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because compressing a media signal; and a set of data from the compressed media signal would improve the entropy per bit which would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

Noll et al. as modified, still does not teach said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

Borza et al. teaches said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 6, lines 5-33).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include said media

signal having the capacity of containing random noise that is completely unpredictable from one moment to the next.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Borza et al. because said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next would produce a random number to be used as a seed in a pseudo random number generator (see Borza et al., column 10, lines 4-12).

As to claims 4, 13, 20, and 27 Noll et al. as modified, teaches wherein:

the compressed data stream includes compression transform coefficients; and the set of data includes a set of compression transform coefficients (see Koopman, Jr., column 7, lines 25-59).

As to claims 5, 14, 21, and 28 Noll et al. as modified, teaches wherein:

the compressed data stream includes data frames of varying length (see Koopman, Jr., column 7, lines 25-59); and

the set of data includes a set of data frames (see Noll et al., column 4, lines 56-67).

As to claims 11, 18, and 25 Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames (see Koopman, Jr., column 7, lines 16-59); and

the selecting step includes the step of selecting one frame of data (see Noll et al., column 4, lines 56-67).

As to claims 12, 19, and 26 Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames and data frame boundaries (see Koopman, Jr., column 7, lines 16-59); and

the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries (see Noll et al., column 4, lines 56-67).

As to claims 16, 23, and 30 Noll et al. as modified, teaches

wherein the media signal includes a noise signal amplitude (see Borza et al., column 5, lines 4-16);

further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude (see Borza et al., column 6, lines 21-33); and

wherein the compressing step includes the step of compressing the quantized media signal (see Koopman, Jr., column 7, lines 1-59).

7. Claims 6, 8, 15, 22, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Koopman, Jr. (U.S. patent No. 5,757,923, and in further view of Borza et al. (U.S. patent No. 6,215,874 B1) as applied to claims 1-5, 7, 9-14, 16-21, 23-28, and 30 above, and further in view of Owashi et al. (U.S. patent No. 6,363,210 B1).

As to claims 6, 15, 22, and 29 Noll et al. as modified, still does not teach wherein:

the compressed data stream includes predictive data frames; and

the set of data includes a predictive data frame.

Owashi et al. teaches encrypting communication signals (see abstract), in which he teaches wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame (see column 9, lines 5-13).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Owashi et al. because wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame would be the most obvious form of compression for video media (see Owashi et al., column 14, lines 29-31).

As to claim 8, Noll et al. as modified, still does not teach wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

Owashi et al. teaches wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats (see column 9, lines 5-13).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, to include wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Owashi et al. because wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats would be the most obvious form of compression for video media (see Owashi et al., column 14, lines 29-31).

Response to Arguments

8. Applicant's arguments filed on 13 May 2004 with respect to rejected claims in view of the cited references have been considered, but they are moot in view of the new grounds of rejection.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

"Using and Creating Cryptographic-Quality Random Numbers" by Callas for teaching "Compression is a randomizing function" on page 2.

"Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients" by Wu et al. for teaching "the higher the compression, the less the redundancy and the more random will the code stream appear" on page 908.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
12 Jul 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100